BlueKeep Vulnerability (CVE-2019–0708)

BlueKeep (CVE-2019–0708) Vulnerability exists within the Remote Desktop Protocol (RDP) used by the Microsoft Windows Operating Systems including both 32- and 64-bit versions, as well as all Service Pack versions:

- Windows 2000
- Windows Vista
- Windows XP
- Windows 7
- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

Possible Attacks

1. An attacker who successfully exploited this vulnerability could perform a Denial of Service (DOS) attack to the target endpoint or the server.
2. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Mitigations

CISA encourages users and administrators review the Microsoft Security Advisory and the Microsoft Customer Guidance for CVE-2019–0708 and apply the appropriate mitigation measures as soon as possible:

- Install available patches. Microsoft has released security updates to patch this vulnerability. Microsoft has also released patches for a number of OSs that are no longer officially supported, including Windows Vista, Windows XP, and Windows Server 2003. As always, CISA encourages users and administrators to test patches before installation.

For OSs that do not have patches or systems that cannot be patched, other mitigation steps can be used to help protect against BlueKeep:

- Upgrade end-of-life (EOL) OSs. — Consider upgrading any EOL OSs no longer supported by Microsoft to a newer, supported OS, such as Windows 10.
- Disable unnecessary services. — Disable services not being used by the OS. This best practice limits exposure to vulnerabilities.
- Enable Network Level Authentication. — Enable Network Level Authentication in Windows 7, Windows Server 2008, and Windows Server 2008 R2. Doing so forces a session request to be authenticated and effectively mitigates against BlueKeep, as exploit of the vulnerability requires an unauthenticated session.
- Block Transmission Control Protocol (TCP) port 3389 at the enterprise perimeter firewall. — Because port 3389 is used to initiate an RDP session, blocking it prevents an attacker from exploiting BlueKeep from outside the user's network. However, this will block legitimate RDP sessions and may not prevent unauthenticated sessions from being initiated inside a network.

In this documentation the DOS attack exploitation will be explained.

Requirements to try this attack

- An attacker machine – Kali Linux
- Attacking Scripts - https://github.com/Ekultek/BlueKeep
- A victim machine – Windows 7

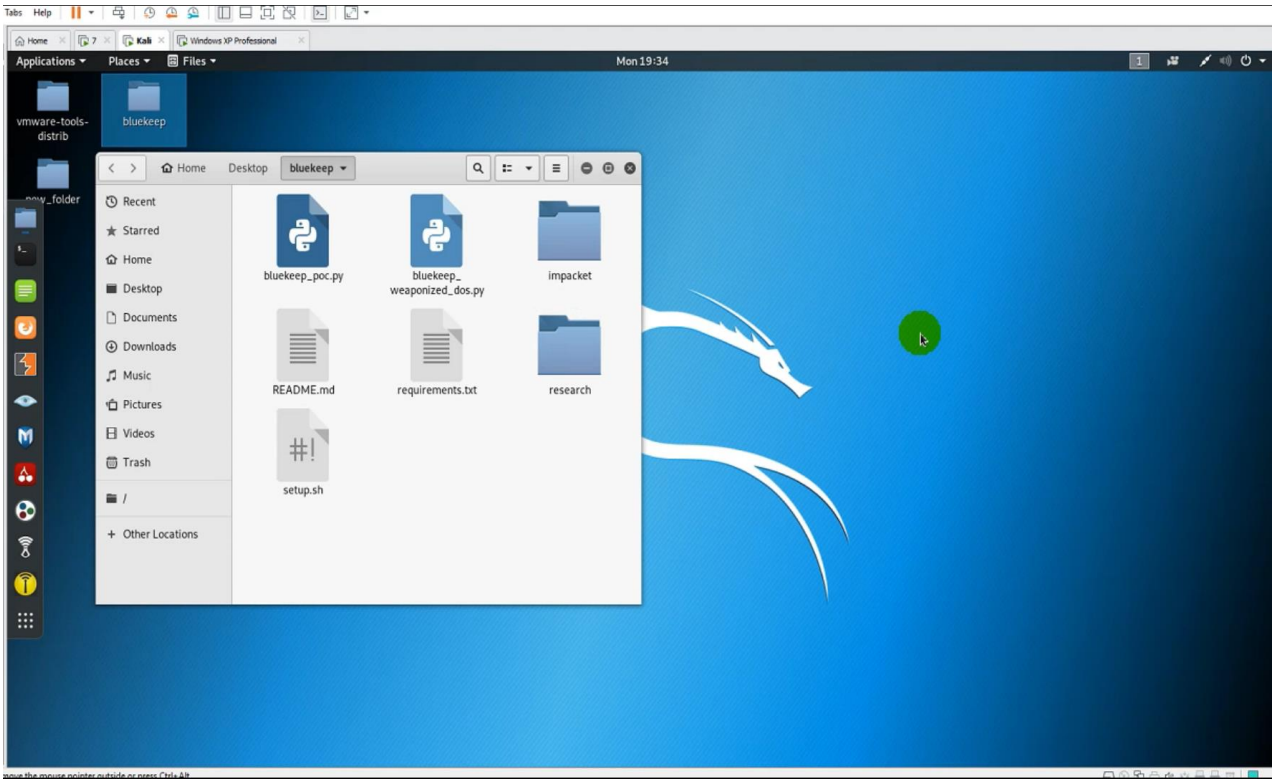
Limitations to try this attack

- The victim machine should have RDP port Open. Port number 3389

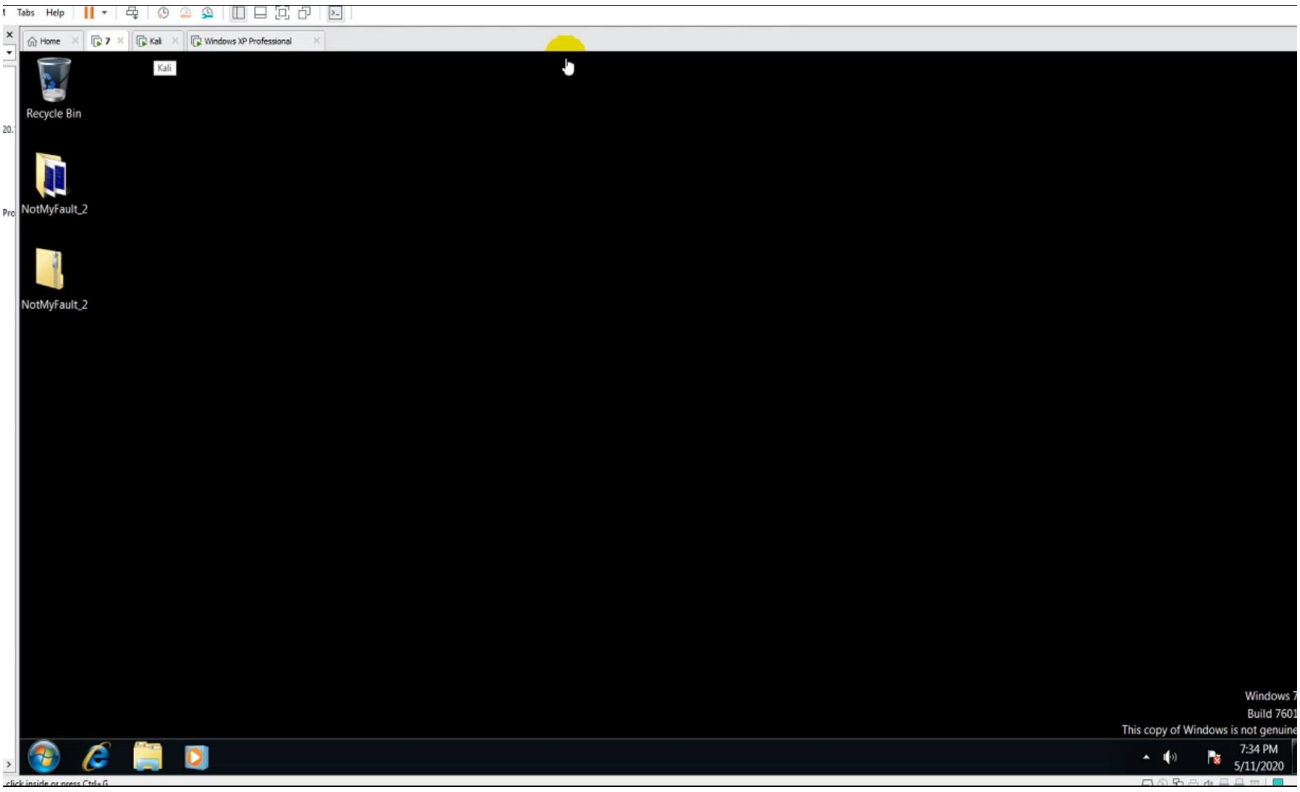
Step by step guide for the DOS attack exploitation

1. Setup the environment

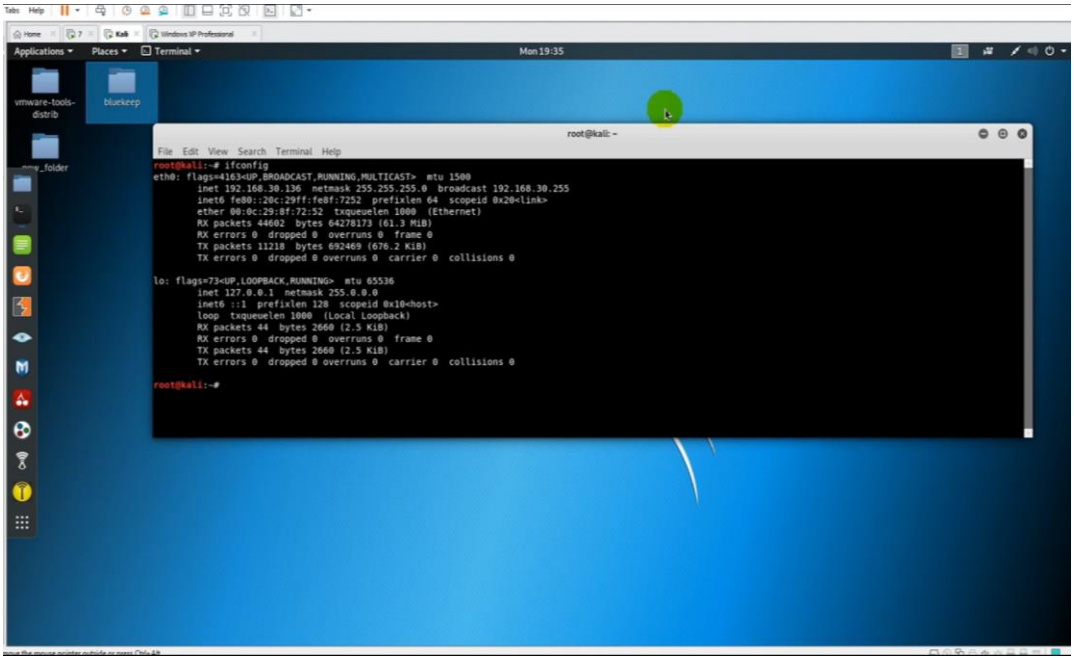
Attacker Machine

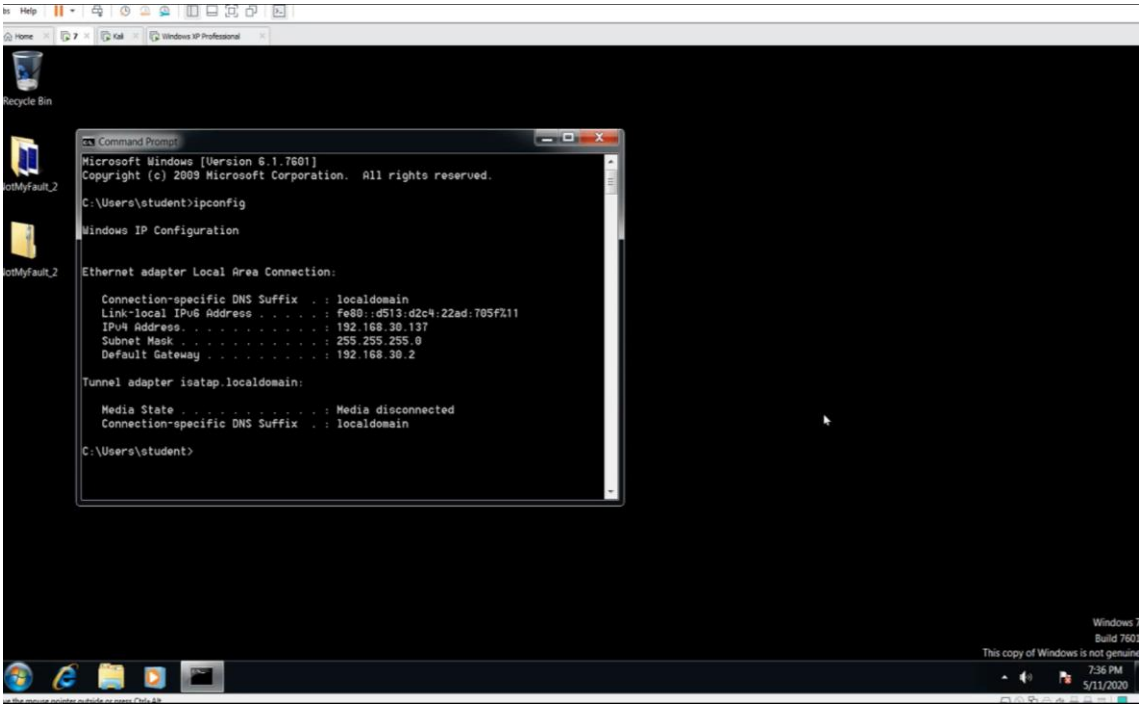


Victim machine

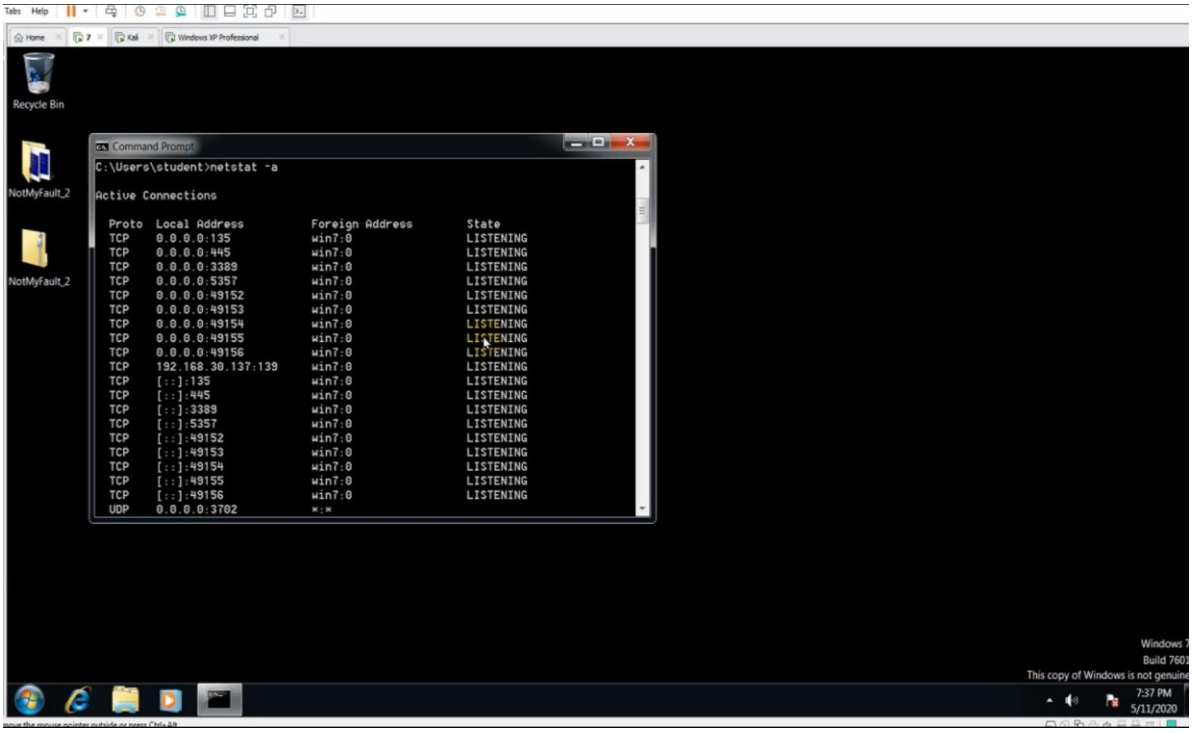


2. Check the ip range in both machines. (both machines should be in the same network)

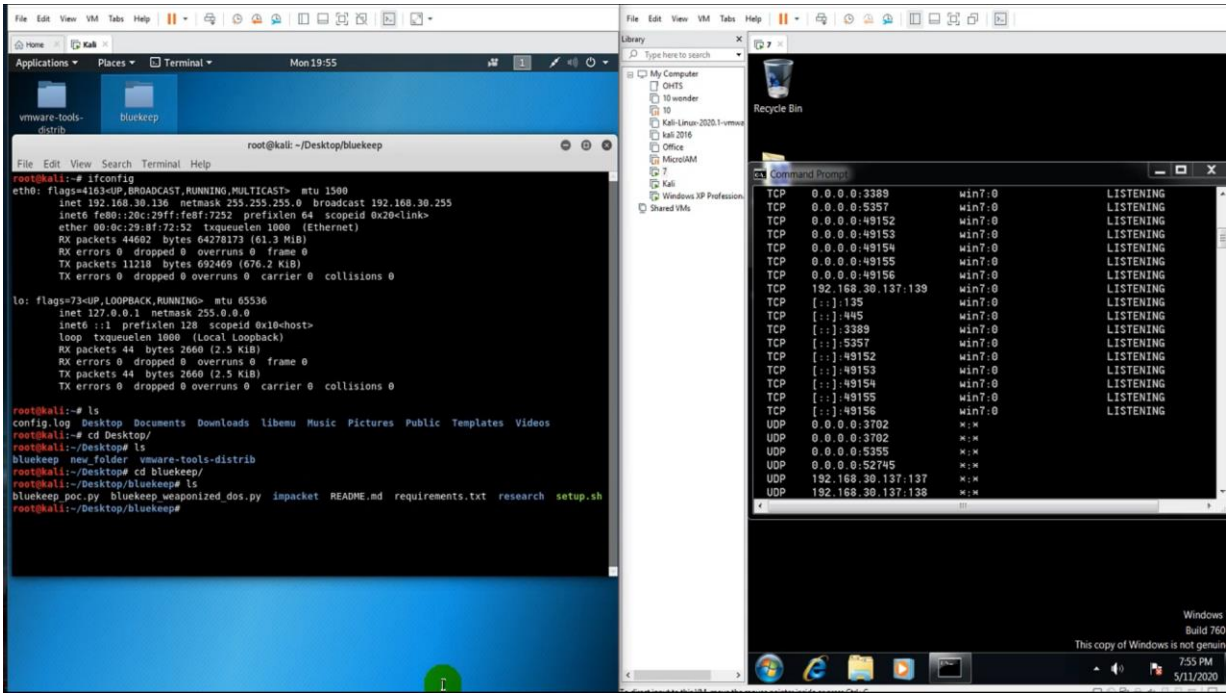




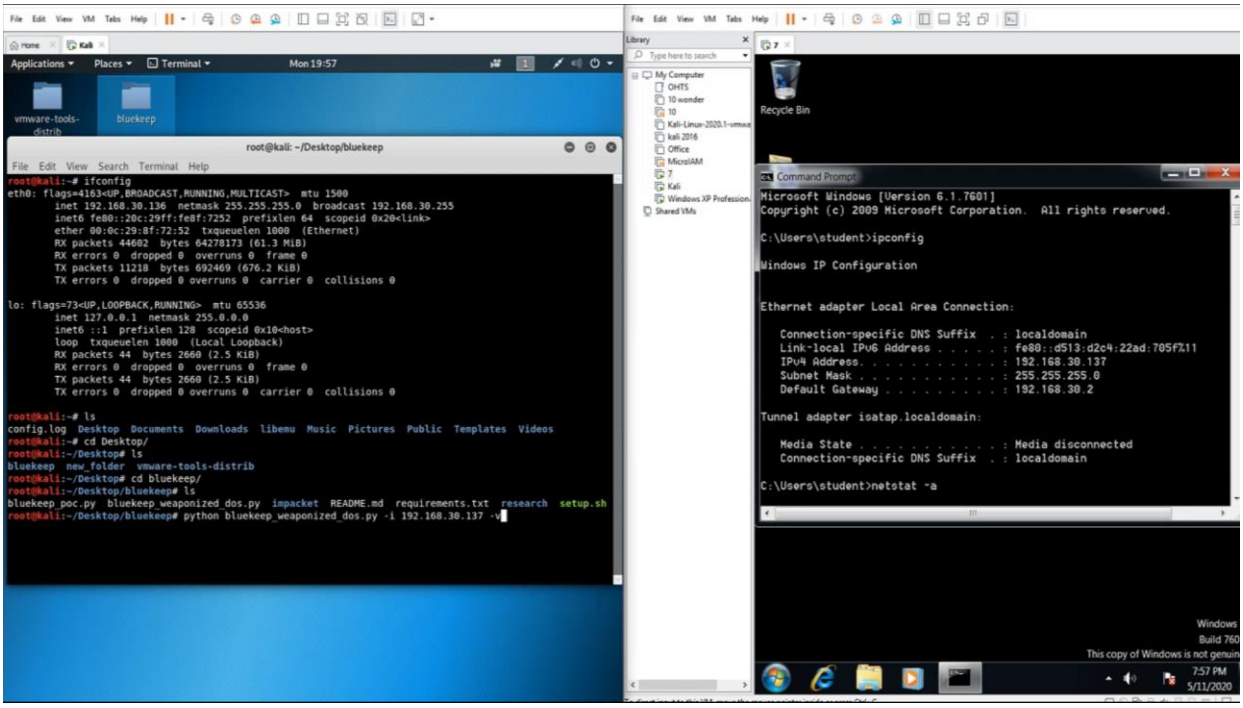
3. Check whether the RDP service is running in the victim machine. (RDP Port Open)



4. Go to the folder where the attacking python scripts are saved.



5. Execute the python script by giving the victim IP address as a parameter.



The victim machine will give a blue screen upon a successful exploitation